CYCRAFT
奧義智慧科技

重掌資安主控權：
2024 台灣企業的外部曝險與內部管理挑戰

資安曝險調查白皮書

為什麼駭客能夠看穿攻擊目標、規劃攻擊，但企業卻難以掌握自身環境，提前設想應對措施？多數網路犯罪組織在攻擊前會進行網路偵察，鎖定疏於外部攻擊面管理的企業。

奧義智慧科技研究團隊在此白皮書中盤點七大風險類別、共 232 項資安風險，發現最嚴重的三大問題為：

1 **95% 企業 Email 服務設定有瑕疵：**
釣魚信件攻擊一直以來都是企業的重大安全挑戰，儘管可以透過教育訓練提高員工安全意識，這仍是治標的解決方法。企業應採取更為治本的措施，如啟用 SPF、DKIM、DMARC 等機制有效防止攻擊者偽冒其網域，以減少釣魚信件。但本次普查結果顯示在 145 個企業組織中，有 138 個組織未正確設置 SPF、137 個組織未正確設置 DMARC，意即在此普查範圍中大部分的企業都沒有正確設定 Email 安全機制。

2 **63.5% 企業資料外洩於暗網：**
普查範圍內共有 3,549 筆資料外洩，以政府機構（平均 87 筆）、電子業下游（平均 26.98 筆）、金融業（平均 21.95 筆）為前三高。政府機構涉及國家安全、公民個人資料、政策制定與其他敏感資訊、電子業富含高科技產品的知識產權，金融業掌握大量個人和企業財務資料，容易淪為勒索軟體犯罪集團的首要目標。

3 **50.8% 企業對外網站憑證有瑕疵：**
在交叉比對近期遭勒索的國外企業與台灣企業後，受駭公司的資安管理敏捷度的確與正常公司有別，以數位憑證相關的類別為例，超過半數遭勒索的企業對外網站憑證有明顯瑕疵，差異極為顯著。

Active Directory 安全白皮書

近年來從美國 Black Hat 黑帽大會到 iThome 臺灣資安大會都持續關注 Active Directory (AD) 資安議題，AD 是企業內部通往其它資源的門戶，負責提供主機與應用程式身分存取與管理服務，隨著組織發展，容易產生諸多不符合現在安全理念的設定，導致 AD 淪為駭客攻擊的首要目標。

在此白皮書中，奧義智慧科技研究團隊揭露了企業 AD 架構中最常見的三大缺失：

1 **84.8% 權限設定瑕疵，導致不當的間接授權：**
多數場域的 IT 人員在新增人員或電腦至網域時，因設定瑕疵而沒有收回 Owner 權限。若新增的使用者或電腦負責 Tier0 帳號或核心系統資產時，IT 人員便會間接獲得預期外的權限，不當的控制關係使存取控制樣態更趨複雜與不易稽核。

2 **隱匿特權帳號高達 26 倍，成為資安死角：**
在此次分析範圍內，每個網域潛在的特權帳號平均高達 2,585 個，是平均網管帳號數量的 26 倍。潛在特權帳號來源很多，如離職員工帳號、已無人使用的服務帳號、或是為求方便的網管秘密小帳。隱匿特權帳號不但是攻擊者入侵內網 AD 最想要的目標，更是資安治理上的陰暗死角。

3 **56% 網域中 ADCS 有提權風險，是攻擊者的最愛：**
根據此次統計，76.3% 企業有使用 Active Directory Certificate Services (ADCS)，其中高達 56% 存在嚴重的提權風險，允許所有使用者將權限提高至網域管理員權限。ADCS 在 AD 中扮演關鍵角色，負責發行用於網域身份驗證的憑證，自 2021 年以來，針對 ADCS 的攻擊手法從 8 種增加到了 14 種，其中以 ESC1 與 ESC4 最為常見，企業應該優先重視這類 AD 風險。

2024 台灣外網曝險盤點

95% 有偽冒風險　**63.5%** 有外洩資料　**50.8%** 有憑證瑕疵

盤點了 145 個單位的曝險分析，包含了上市公司、重要政府與醫療機構，特別針對曾被勒索軟體攻擊過的單位，掃描外網與暗網曝險情資。

了解外部曝險及先兆事件是預防資安風險的關鍵。奧義智慧科技的 XCockpit 可依照 CTEM 框架協助企業評估資安態勢，持續監控外部潛在威脅。
本白皮書針對政府機關、傳產企業、電子產業上、中、下游以及醫療產等六大產業提供了常見風險、技術解決方案及管理策略建議。企業可根據自身曝險情況選擇適當解決方案，制定改善計劃，有系統地降低曝險風險。

2024 台灣 AD 安全大普查

84.8% 權限設定瑕疵　**26倍** 的潛在特權帳號　**56%** ADCS 可以提權

普查了 27 個上市公司、重要政府與醫療機構，涵蓋了 46 AD Domain，總共包含了 105.7 萬物件。其中 Domain 的規模最大高達 23 萬的帳號，而中位數約 7,438 個物件。

此份白皮書除了針對上述 AD 權限設定問題與新興攻擊有詳盡的分析，也論及雲端混合身分驗證、密碼管理政策、AD 基本設定強化等管理面向。我們建議先分類、識別出應優先保護的核心資產，分析各物件與帳號關聯，持續監控潛在的攻擊路徑。借助奧義智慧科技 XCockpit 的自動化 AD 物件權限修正腳本、攻擊路徑視覺化模擬等功能，不僅可減輕 IT 與資安團隊的管理成本，更有助企業直觀且精準劃定內在的攻擊構面。

奧義智慧科技研究團隊耗時 7 個月，深入研究台灣近 200 家上市櫃企業、重要政府單位及醫療機構，探討了資安的現況與挑戰。我們專注三個關鍵議題：企業外部曝險、內部 Active Directory (AD) 管理設定，以及紅藍隊演練評估，在白皮書中詳述各議題的風險原因、案例分析、技術手法與應對建議，提供台灣企業在資安防禦策略上的重要參考的依據。

紅藍隊演練白皮書

目前主管機關與企業法規中，已將紅隊演練列為每年資安重要的任務。奧義智慧科技作為藍隊一方，也與企業資安團隊合作，觀測了多場大型的紅隊演練，彙整攻防的數據，協助評估演練效果。

奧義智慧科技研究團隊透過此白皮書，建立具通用性的分析標準，嘗試客觀判斷不同的紅藍隊演練成效，歸納出三大重點：

1 **企業比預期中還脆弱，平均 1.3 天打進第一台端點：**
紅隊成功入侵企業的時間遠比預期地短，平均 1.3 天可攻下內網第一台端點。更出乎意料的是，超過 50% 場演練在第 1 天基本上已掌握內網的所有設備，約 80% 場演練在 3 天內就完成全場域入侵，顯示企業的防禦普遍而言相當脆弱。

2 **內網權限為兵家必爭之地，平均 3.5 天取得 AD 權限：**
紅隊演練在初步取得立足點後，會開始尋找各種提權管道，滲透內網並擴大衝擊。我們分析的每一場演練裡，紅隊都會攻擊 AD 以控制網域，平均 3.5 天取得 AD 權限，甚至有 30% 的案例在 1 天內就可控制內網，最晚也不超過 7 天。對紅隊來說，不論是取得單台機器的 Local Admin、或藉由 AD 拿下全網域的特權帳號，都易如反掌。

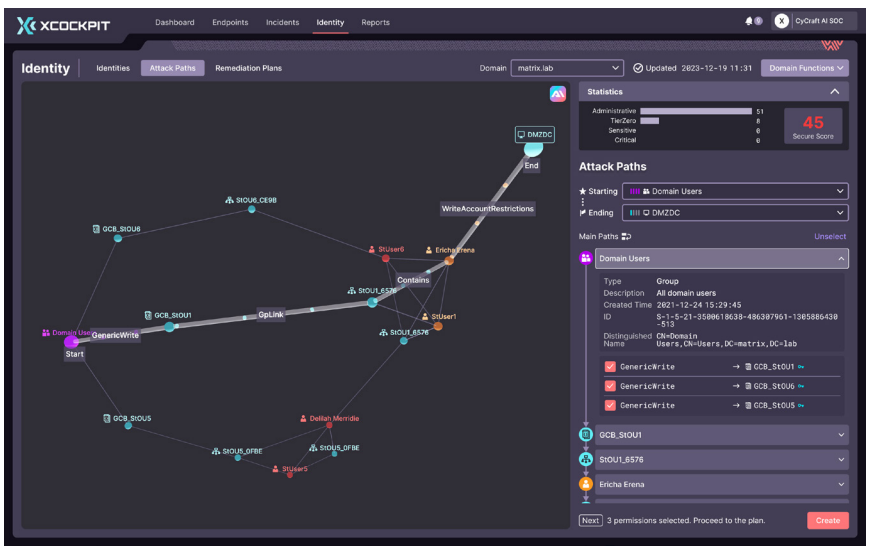
3 **紅隊演練測試範圍有限，平均控制 18.5 台電腦：**
此研究顯示，企業多將紅隊演練當作資安健診，無法最大化攻擊演練的真正效果。由於演練時程普遍有限，每場演練平均僅入侵 18.5 台電腦，我們建議企業應將紅隊演練著重於攻擊路徑的驗證，探索新的攻擊向量、攻擊路徑，而非藉由紅隊演練企圖獲得全面性的安全風險評估。

在紅隊演練白皮書中，我們觀察到每一場演練都可滲透進內網，幾乎每場演練也都提權至網域管理權限，顯示了企業普遍在權限管理、IAM 議題上仍有不足。紅隊演練除了可揭露潛在漏洞，企業也應藉此衡量藍隊服務的應變速度與整體績效。在我們參與的演練中，奧義智慧科技 XCockpit 可集縮約 98.2% 的高風險事件、縮短平均偵測時間 (MTTD) 至 2.1 分鐘，透過 BlueTeam AI 自動服務將上千件的告警輕量化、快速化，強化資安團隊產出至人力可負荷範圍。

結論

有鑑於白皮書揭示的企業外部曝險難以掌握、內部身份驗證管理複雜、資安機制績效不易評估等問題，奧義智慧科技 XCockpit 自動化威脅曝險管理平台整合了外部攻擊面、AD 特權帳號與端點安全的管理，在單一平台上提供即時端點威脅監控、各項風險指標量化、案情報告自動產出等服務。輔以專屬的生成式 CyCraft AI，XCockpit 打造了人類與 AI 混合編隊的新世代解決方案，依循 CTEM (Continuous Threat Exposure Management) 框架，強調預視攻擊面 (Attack Surface)、奪回資安戰場主動權。根據我們的實績數據，此人機合作的新型態資安團隊，可提高資安團隊產能 20 倍、提升值班資安人員告警處理效率 42 倍，能有效、精準、快速強化企業資安韌性。

過去我們僅能消極回應攻擊，但現在有了自動化工具，就能積極劃定戰場疆界、主動管理攻擊面，進而預視潛在攻擊路徑和反制方法。奧義智慧科技 XCockpit 透過量化企業內外風險、透視組織安全，落實主動防禦概念與措施，賦予各界無懼未來資安挑戰的防守能力。



XCOCKPIT
CyCraft AI Copilot

關於奧義智慧科技

奧義智慧科技（CyCraft Technology）是一家專注於 AI 自動化技術的資安科技公司。成立於 2017 年，總部設於台灣，在日本和新加坡均設有子公司。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。

自創立以來，致力於透過 AI 自動化技術解決資安產業長期面臨的各種挑戰。我們團隊擁有豐富的資安事件調查經驗，並深入研究人工智慧技術，將 AI 與機器學習技術應用在資安實務中，研發出自動化的資安威脅管理與調查平台。我們整合了端點偵測與回應、特權關聯衝擊分析、外部攻擊面管理等防禦機制，提供全方位自動化資安防護，協助資源有限的企業實現資安韌性。

contact-tw@cycraft.com
+886-2-7739-0077