CYCRAFT WHITE PAPER

CYCRAFT

為什麼你的 Active Directory 防護無法成功阻擋駭客？

解析常見 AD 安全措施與防禦有效性

2024.05

前言

長久以來，Windows Active Directory (AD) 做為廣受採用的身份驗證與管理工具，掌管著企業網路場域許多重要關卡的鑰匙，然而其悠久的歷史與高度複雜性，卻也無可避免地導致了許多易被攻擊的弱點與漏洞，並成為現代 APT 攻擊中，駭客最常利用的攻擊途徑之一。於此同時，企業中的 AD 管理人員，若對 AD 內部運作原理有所誤解或迷思，也很可能造成難以估量的巨大風險危害。

可能造成 Active Directory 資安破口的因素多不勝數，如不安全的群組使用、帳號權限過高、帳號委託濫用、網域狀態任意複製、未導入密碼安全政策、未採用敏感帳戶保護等，面對 AD 這項須重點保護的關鍵核心資產，資安人員應更積極、謹慎規劃管理方式，瞭解駭客如何利用 AD 弱點進行入侵、進而奪得網域控制權，才能相應地建立正確的應對方式，面對無處不在的駭侵攻擊。

本文將針對 Active Directory 在 IT 管理中的重要性、駭侵攻擊手法、常見安全措施進行介紹，並解析各個防禦方式的應用情境與有效性，幫助您更清楚應如何建立有效、確實的 AD 資安防禦措施，在資訊戰的猛烈砲火中，限縮網路邊界、開闢出一條安全之路。

奧義智慧 XCockpit Identity 帳號安全態勢管理

奧義智慧的 XCockpit Identity 帳號安全態勢管理，是由熟悉 AD 內部原理的資安專家與 AI 人工智慧聯手出擊，並整合端點偵測與 AD 物件盤點，完整分析靜、動態資料並進行可視化，AI 自動化繪製企業網路場域中潛在的駭侵路徑圖，協助企業評估盤點 AD 設定弱點、對症下藥解決牽一髮動全身的 AD 安全隱患。

XCockpit Identity 帳號安全態勢管理特色：

- 深度探索：分析並可視化 AD 物件間的異常關係
- 專家知識：盤點 AD 設定弱點與常見潛在安全問題
- 智慧分析：偵測潛在虛擬群組與隱匿的高權限帳號
- 模擬紅隊：智慧化計算可能攻擊路徑，模擬紅隊攻擊
- 資安健診：評估並量化 AD 環境整體資安風險
- 防禦策略：提供強化 AD 策略，限縮資安威脅邊界

為何 AD 是兵家必爭的資安核心資產

鑒於歷史性與 Windows 系統的高市佔率，與 Windows 系統間擁有高相容性的 AD 同樣有著高度普及的特徵；而在實際使用上，為了達到政府組態基準 (Government Configuration Baseline, GCB) 的合規，許多的 Windows 安全設定，也能透過群組原則物件 (Group Policy Object, GPO) 派送的方式來快速套用，或利用 GPO 針對大量電腦進行軟體安裝、相關設定等，對企業而言具有顯著的便利性這一大優勢。

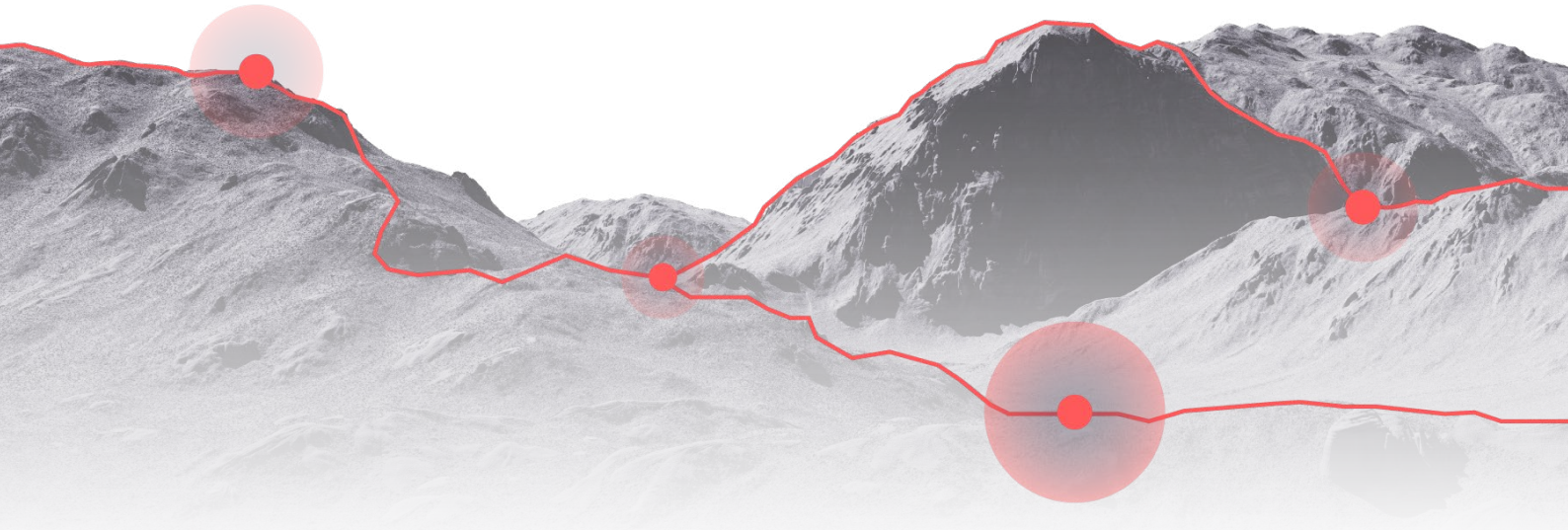
然而，便利性的背後往往也帶來暗藏的風險，在網路世界之中，掌管著存取權的 AD 及其「身份驗證」功能，就如同鑰匙之於保險箱一般，佔據著無可替代的重要地位，一旦駭客成功攻擊並加以利用，便可以扮演企業內的特定人物，做到許多諸如派送惡意軟體、修改存取權限、竊取資料等影響廣泛的惡意操作，而這些可能使企業蒙受巨大損失的行動，甚至不一定需要 AD 內的最高權限、也不一定得要攻下網域控制站 (Domain Controller, DC) ，而是只要針對駭客想執行的目標，取得特定的部分權限憑證即可。

更有甚者，一旦駭客順利攻打下 DC，那麼 AD 本身與許多企業常用服務相互掛勾的特性，便可能成為駭客的可趁之機，藉此連結到其他欲駭入的目標服務中。總上所述，AD 在企業網路場域中的高市佔率、長年以來人們對 AD 累積的依賴，以及其內部設定的複雜性，種種因素造就了 AD 在資訊戰交鋒中關鍵的戰略地位。

駭客如何「合法」利用 AD 駭入您的內網

駭侵威脅甚囂塵上，企業對於單位內資產的資安防護也愈趨完整，多數企業針對 AD 等核心資產皆會設下重重防禦措施，包含特權帳號管理、定期修補漏洞等，然而，為何駭客仍然能成功攻入企業呢？知己知彼方能百戰百勝，掌握駭客常見的入侵方式，也是強化應對能力、有效解決威脅的關鍵之一。

本章節將帶您瞭解駭客是如何取得權限，並「合法地」在您企業的內網中穿梭自如。



濫用特定帳號修竄改存取控制列清單

AD 中的自由判別式存取控制清單 (Discretionary Access Control List, DACL) 扮演著十分重要的角色，DACL 記錄著各個使用者或系統行程對物件的存取控制權限，並且是由許多存取控制條目 (Access-Control Entry, ACE) 所組成的列表。DACL 存取權限的設定一旦發生錯誤，或因便宜行事而輕率進行設定，例如管理群組權限設定過高、為使用方便而直接給予特定帳號高權限等，便很有可能成為駭客利用的破口。

擁有修改或管理 DACL 清單權限的使用者，不一定同時擁有物件的存取權限，然而由於該使用者能夠修改 DACL，便可以將自己所擁有的權限進行調整，使自己獲得特定物件的存取控制權。而這一特徵的背後同時也代表，駭客事實上不需要直接駭入原先就具備高權限，因此受到嚴密保護的重要使用者，若駭入防備較鬆散的 DACL 管理者帳號，一樣有機會透過改動 DACL 內容的方式，讓自己擁有目標物件的權限，是一般企業管理 AD 時容易失誤的盲點。

舉例而言，常見的 DACL 設定中，可能會將 AD 的維運人員設置成可以對特定組織單位 (Organization Unit, OU) 內的使用者進行密碼重設，雖然這是個乍看之下相當合理的設定，不過若該 OU 之中，包含了高權限的重要帳號，那麼駭客就可以利用維運人員，重設高權限帳號的密碼，並藉此成功達到提權的目的。因此，若是產品背後邏輯由熟悉駭客思維的資安專家協助，針對攻擊者容易利用的權限關係，進行一次深入完整的盤點，對組織 AD 健康狀態的強化，便會有著顯著的幫助。

共用主機造成的憑證竊取與 Relay Auth 風險

凡走過必留下痕跡，在數位世界中亦然，在進行資安事件調查時，就像現實中辦案會採集指紋一樣，往往會透過蒐集「數位足跡」加以抽絲剝繭。相反地，曾經在某台機器中活動過的痕跡，不只對資安人員查案有幫助，也可能成為駭客利用來做為盜竊憑證等的入侵手段之一。

透過遠端桌面協議 (Remote Desktop Protocol, RDP) 或虛擬桌面基礎架構 (Virtual Desktop Infrastructure, VDI) 可以讓不同的人在任意時間地點共用同一台主機，使得許多操作與管理更加方便；然而，這樣的做法也有致命缺點，便是有可能會留下足跡，讓惡意攻擊者得以利用。因此，同時開放了較多帳號可登入的 RDP 主機，相對也較容易被做為攻擊途徑。

如同前段提及，多個使用者共用同一台主機，難免會留下可被利用的數位足跡，導致駭客攻擊事件的發生。透過 mimikatz、Rubeus、WCE 等工具，駭客得以進行憑證轉儲 (Credential Dumping) ，進而偷取並偽裝他人的身份，長驅直入進到企業系統之中，甚至嘗試提權或橫向移動，擴大對網域的控制，以執行如派送勒索軟體、盜竊機敏資料或更多惡意操作。

此外，使用者無法得知機器中的其他帳號是否為安全、合法的使用者，所以也會存在著與駭客同時共用主機，故而引發 Cross-Session 攻擊的可能性。利用 Windows 設定的 Cross-Session 缺陷，以及衍生的 KrbRelay、RemotePotato0、Lsarelayx 等新型攻擊工具，攻擊者便有機會在對方不知情的情況下，讓同時間登入於相同機器的使用者帳號，向其他服務申請驗證，進而偷取驗證進行 Relay Auth 攻擊，擴展其在系統中的操作權限範圍。

未能正確掌握影響整體場域安全的核心資產

AD 攻擊來勢洶洶，對資訊安全有所重視與警覺的企業，理所當然地會投入成本去強化 AD 的安全性與防禦措施，然而，考慮到 AD 本身的複雜性，以及企業採用 AD 多年來所累積的各項設定，若負責 AD 的人員未確實掌握交接細節，抑或是不夠熟悉 AD 特性，便很有可能無法正確圈出需加強防禦、能影響到整體場域安全的那些「核心資產」。

舉例而言，AD 憑證服務 (Active Directory Certificate Services, ADCS) 便是一種易被忽略的核心資產，ADCS 時常被當作應用公開金鑰基礎架構 (Public Key Infrastructure, PKI) 來發憑證的伺服器，而人們卻常忘記發出的那些憑證可以用在 AD 身份驗證上，因此事實上 ADCS 也能夠影響到整體場域的安全。

由此可見，未正確掌握所有核心資產的這件事情，本身即為一個相當明顯的弱點。試想若企業設置了 AD 核心資產的保護措施，卻無意間漏掉了那些不同層級資產的防禦，因此控制措施並未確實地套用到所有核心資產上，那麼即使強化了防禦，有重要項目沒被完整覆蓋到，對駭客而言也仍然有能加以利用的弱點與可趁之機。

在真實的服務案例之中，便曾出現過這樣的情況，客戶認知為核心資產的主機僅有 10 台，而盤點出來卻有 20 台之多。由此可見，採用納入了真正熟悉 AD 結構、瞭解駭客攻擊手段的資安專家意見所設計出的服務，來為企業盤點 AD 核心資產，才能更有效便捷地解決這項問題，而企業也可藉此機會重新盤查一番，提升對內部資產、設定與架構的掌握度，避免類似問題一再發生。

為何常見的安全措施不足以應對所有現代駭侵威脅

隨著近年來攻擊事件頻傳、駭侵手段不斷地進化，資訊安全的重要性已不再是個需要多加解說的事情，企業對於資安防禦的重視程度持續提升，其中，作為兵家必爭之地的 AD 自然會是企業著重防禦、設下層層措施的標的。

然而，為何企業明明已經加強防禦了，AD 攻擊事件卻仍頻傳？防禦產品與安全措施的選擇，或許是最大的影響因素。本章節將從四種常見的 AD 安全措施出發，帶您探討為何它們並不足以應對所有的現代駭客攻擊。

定期更新修補 AD 漏洞

關於 AD 的資安漏洞時有所聞，其中也不乏如 Zerologon（漏洞編號 CVE-2020-1472）等，在通用漏洞評分系統 (Common Vulnerability Scoring System, CVSS) 被評為滿分 10 分、破壞力與影響範圍皆不可小覷的高風險漏洞，而藉由這些漏洞，駭客可以更簡單地取得 AD 中高權限的身份。

每當有重要漏洞被挖掘出來，不只駭客們會爭相開始進行大範圍的掃描與攻擊，企業也會在第一時間著手應對、進行改善或安裝官方提供的修補檔等，這當然是正確且有效應對漏洞的方式；然而，漏洞的修補與更新永遠不會有結束的一天，而許多時候 AD 系統的弱點，並不一定是漏洞所導致，也不一定能被修補，甚至於，部分驗證機制本身的弱點可能無法緩解，而假設企業的 AD 安全設定有問題，駭客其實不需要利用漏洞，也有機會成功入侵。

此外，Microsoft 在處理重大更新時，可能會採取多階段實施的形式，部分更新需要使用者主動啟用，或者在更新發布的半年至一年後才強制啟用，這種多階段實施的做法主要是為了避免更新所造成的使用者服務中斷，因此，僅執行更新而未留意細節，很可能並未真正啟用安全措施。以編號 CVE-2021-26414 漏洞為例， Microsoft 在 2021 年 6 月 8 日釋出了對應的更新修補，但該次更新內容事實上僅為支援緩解，對於伺服器的系統卻並未強制啟用，而是到 2022 年 6 月 14 日的安全性更新才預設為啟用，所以 CVE-2021-26414 直到當時才正式因更新而消失。

另一方面，也並非所有機器都能安裝修補，像是 Windows 系統上兩大驗證機制 NTLM (New Technology LAN Manager) 和 Kerberos 中，NTLM 原先的設計並沒有包含加密保護，而是到了後期才推出緩解機制，也因此基於場域相容性等因素，不是所有情境都能適用後續推出的機制，例如部分作業系統版本較舊的機器就沒有支援。

採用特權帳號管理軟體

為了強化重要核心資產的防護，許多企業往往會為手握大量權限的「特權帳號」，設下較為嚴密的防禦措施，如採用額外的特權帳號管理軟體等，然而，僅僅是使用特權帳號管理服務，對抵禦現代駭客攻擊而言卻仍是不夠的。特權帳號管理的方式，主要有附著於 AD 之上、替 AD 套上一層身份驗證功能的，或者獨立於 AD 之外向第三方服務進行帳號驗證。這兩個種類，使用者可以透過這些套在應用程式的服務，對特權帳號進行控管。

多套用一層身份驗證的作法，固然提升了登入的安全程度，但實務上，若駭客已經藉由上述其他入侵手段，成功竊取到特權帳號的憑證，那麼當駭客要偽裝成該特權帳號使用者時，便不需要再經過特權帳號管理的軟體進行登入，如此一來，該軟體就無法達到有效遏止駭客入侵的目的。此外，特權帳號管理軟體一般而言，會在 AD 上註冊一個高權限的帳號，用以執行所需的管控措施，但此帳號也有可能成為駭客的攻擊標的，建議使用時多加謹慎留意。

在 AD 安全防護這方面，許多情境下的盲點與癥結點，在於管理者忽略了駭客入侵採取的可能是「合法手段」，諸如利用特定使用者憑證合法登入並操作，或是進到系統後合法地修改部分權限設定等，因而並未設置對應的防禦措施。更全面且穩妥的 AD 防禦，需要將駭客的合法入侵手段一併考慮進去，除了一般常見的弱點和漏洞盤點外，也須盤查高權限、高風險的帳號中，是否有不合理的存在或可疑的行為。

強化密碼並導入多因子驗證

考慮到駭客入侵的風險，許多企業也會針對密碼規則進行強化，甚至導入多因子驗證 (Multi Factor Authentication, MFA) 來加固登入的安全性，然而，正如同前述曾提及過的，若駭客已透過其他手段成功獲取憑證，那麼便不需要再經過登入的程序、可以直接進行操作，自然也就不需要理會 MFA 機制。

即使撇開 MFA 機制是否有效的議題，單純考慮到安全機制是否完整涵蓋到所有服務的這一點，確實也會有一些服務並不被納管在特權管理或 MFA 機制之下。舉例而言，有些特權管理系統僅在人類使用者操作的步驟，會要求執行 MFA 驗證，像是 PsExec 或 WMI (Windows Management Instrumentation) 等 IT 人員常使用的管理工具，便不需要經過 MFA 驗證；此外，在系統背景執行的服務，一般也不會使用到 MFA，正因如此，依靠 MFA 機制對於 AD 安全性的提升，效果可說是十分有限。

至於強化密碼規則的做法，也同樣有著相似的問題，並且在 AD 的攻擊手法裡，駭客通常並不會仰賴暴力破解密碼的方式，來達到入侵的系統目的。比起從外部替登入機制套上一層又一層的防護，深入盤查 AD 內部的入侵途徑、處理掉駭客攻擊最可能運用的弱點，才是更能一勞永逸、有效解決威脅風險的方式。

執行資安健診或顧問諮詢

多數不熟悉資安領域的企業，會選擇找廠商執行所謂的資安健診或是顧問諮詢服務，可以想見，像是健診服務中常做的項目稽核、帳號盤點等，當以合規做為主要目的，或在某些特定的情境下，的確有著良好顯著的功效，但這些服務往往並非以攻擊者角度進行，也不會涵蓋到入侵途徑等更深層的部分，在防治駭客威脅的這一部分，能達到的助益便十分有限。

本章節中所介紹的幾種 AD 安全對策，都有各自特定的效用、也有各自的弱點，防禦產品本身沒有對錯之分，但是有合適或不合適的應用場域；清楚界定欲解決的問題、定義導入防禦措施的目的，才是企業真正對症下藥、找到有效解決方案的一大前提。

透過入侵路徑分析徹底限縮網路邊界
XCockpit Identity 帳號安全態勢管理

為解決企業重視的 AD 入侵風險問題，奧義智慧專家團隊研發 XCockpit Identity 帳號安全態勢管理，整合原有端點偵測與回應 (Endpoint Detection and Response, EDR) 產品在端點上蒐集的動態資訊，以及深入的 AD 帳號資訊盤點，AI 自動化分析帳號關係、管理架構，並將 AI 模擬預測的潛在入侵路徑與機率，進而繪製出可視化的場域圖，幫助企業量化網路威脅邊界、評估如何設置最有效的防禦措施及攻擊斷點。

奧義智慧 XCockpit Identity 帳號安全態勢管理主要功能與服務項目如表所示，與市面上多數 AD 盤點產品相較之下，不僅擁有更加完整、詳細的分析項目內容，更是由具多年攻擊事件實務鑑識調查經驗的專家團隊，以駭客思維的角度做為切入點，所設計出貼合真實資訊戰場應用情境的服務。量化潛在威脅以利量測防禦痛點，進而最佳化地限縮 AD 網路邊界，確立安全無虞的場域環境。

AD Visualization 可視化關係圖	分析 User、Computer、Group、OU、GPO 等多種 AD 物件，繪製可視化的物件關係圖，幫助企業網管人員一目了然地快速掌握場域態勢。
AD Security Posture 安全態勢評分	自動化量化與量測各項 AD 物件設定與場域內帳號安全性，評估企業 AD 安全體質分數，協助企業快速判別資安績效指標。
Xensor EDR Integration 端點資訊整合	整合奧義智慧 Xensor EDR 解決方案，納入 Event Log、Login Session 等端點動態資料，補強 AD 中資訊不足之處，以進行更全面性的潛在入侵途徑分析，並可即時偵測告警、第一時間反應惡意行為。
Administrative Accounts 特權帳號分析	以獨家 CyCraft AI 技術結合專家實戰經驗，深度挖掘企業單位 AD 內的高權限網管帳號，如潛在虛擬群組與隱匿的特權帳號等，為企業分析難以覺察的權限管理問題。
Attack Path Simulation 入侵路徑模擬	利用 CyCraft AI 演算法技術，全面性分析 AD 中逾 35 種帳號與權限關係，智慧化模擬駭客攻擊，計算所有可能的駭侵攻擊路徑與機率。
Account Assessment 帳號設定盤點	執行多種專家分析模組，盤點密碼存取屬性、高風險屬性、服務帳號屬性、網域特殊權限、ADCS、LAPS、SPN、AS-REP Roasting、DCSync，以及不建議的 Owner、群組規劃、權限設定等常見安全問題。

XCockpit Identity 的運作原理

AD 中預設皆為可搜尋的公開資訊，例如存在哪些物件、帳號間的關係、帳號與物件間的管理權限等，藉由這些資訊可以進行詳細的盤點與分析，檢視企業 AD 內部的是否存有安全隱患，像是權限設定是否與預期相符、是否有過多的 Shadow Admin 帳號等。

由於 AD 本身高度的複雜性，導致了即使所有資訊在 AD 中皆為公開狀態，但一般企業 IT 或網管人員不夠瞭解 AD 設定細節、也不清楚哪些是高風險的重要資產，因此，事實上企業很難自行找出檯面下隱藏的弱點，並完成真正有效的盤點。舉例而言，Account Operators 和 Backup Operators 在 AD 中原本是用以重設密碼、備份系統的帳號，但多數的資訊人員不曉得，這兩種帳號也能夠影響整體網域的權限。

此外，奧義智慧將 AD 靜態資料分析與 EDR 產品 Xensor 在端點上蒐集的動態資料進行整合，以便更加深入、全面地分析 AD 安全弱點與模擬駭客入侵路徑。雖說 AD 中資訊為公開狀態，但仍有諸如 Logon Session、Running Process、Event Log、Local Admin Group Member 等部分資訊，必須要在當台端點的機器上才能進行查詢、無法透過 AD 公開資訊來得知，而這些 Local 端資料正是掃描端點後能幫助我們更準確進行分析評估的重點所在。

舉例來說，透過端點中的動態資料，有機會發現到 Local 設定允許特定使用者帳號登入該端點，或是從 Logon Session 中得知特定帳號曾經在這台端點中出現，如此一來，便有可能在端點上針對該使用者進行 Credential Dumping，進而竊取憑證後偽裝成特定使用者，並進入系統中執行惡意的操作或試圖提權。

考慮到這點，奧義智慧的 XCockpit Identity 服務將動靜態資料互相結合，為企業提供完整且準確的 AD 安全分析盤點與入侵路徑模擬，並以專利 CyCraft AI 技術將潛在入侵途徑等資訊可視化，繪製出涵蓋企業整體網路場域的路徑圖，協助企業定義網路邊界、找出最可能遭受入侵的路徑並加以修復截斷。此外，Xensor EDR 系統也會同時偵測端點的異常行為，在端點遭駭時立即發出告警 (Alert) ，讓企業得以在第一時間迅速做出應對。

XCockpit Identity 的執行方式

首次採用並執行 XCockpit Identity 服務的企業，若原先並非奧義智慧 Xensor EDR 解決方案客戶，可從 AD 靜態資料盤點與分析開始，先單純就高權限帳號數量、物件關係盤查、設定弱點檢視等僅需 AD 公開資料，且無須開通任何高權限帳號便可進行的事項展開調查，初步了解企業 AD 安全體質概況。

若企業已擁有 Xensor EDR 或欲擴大部署、涵蓋更完整的 AD 分析報告，則可進一步掃描蒐集端點動態資訊，補充如帳號活動軌跡、憑證是否殘留等內容後，執行進階攻擊手法的調查，以及最重要的入侵路徑模擬與評估。奧義智慧的資安分析師與 AD 專家將協助您了解報告書的內容，並提供整治、強化方向的策略性建議。

隨著企業內部的變動及操作使用，靜態、動態資料事實上都會隨時發生更改，因此建議企業在首次完成 XCockpit Identity 服務的分析後，規劃每季或每半年定期執行一次盤點，確保 AD 資安體質持續維持在足夠強韌的良好狀態。另外，若有重大服務上線、較大規模的人員異動時，也建議可額外安排一次 XCockpit Identity 盤點服務。

XCockpit Identity 的獨特之處

奧義智慧 XCockpit Identity 服務納入端點安全概念，不同於多數傳統方案只以安全設定檢查作為目標，且相較於部分僅利用網路層 Protocol 蒐集資料的攻擊路徑分析服務，奧義利用自有的端點偵測產品 Xensor 蒐集動態資料，可以減少雜訊的影響並達到更高的精確度；利用獨家 AI 技術繪製可視化物件關係圖表，幫助企業輕鬆了解潛在入侵路徑與其機率性，能更簡單、清晰地掌握網域的場域態勢，決定整治措施和先後順序。

於此同時，奧義智慧 Xensor 端點安全系統的部署具高度彈性、輕量化的特徵，且可跨作業系統平台，視情況部分調查內容不需要網域控制站 (Domain Controller, DC) 權限便可進行，與多數產品須開啟高權限才能執行不同，減少相應的安全風險、降低企業導入 XCockpit Identity 的困難與成本。

XCockpit Identity 服務涵蓋企業場域，完整盤查並分析整體間的關聯性，而非僅檢視單一端點上的設定資訊；此外，XCockpit Identity 不只是模擬入侵特定目標的最短路徑 (Shortest Path) ，而是以獨特的 AI 技術找出所有可能的路徑，能以駭客思維進行危險程度排序並逐一破解，劃出需優先守護的網路邊界，有效提升 AD 體質改造的實際成效。

結語

本文從 AD 的安全威脅切入，介紹多種常見防禦方式的優缺點，並帶您認識奧義智慧 XCockpit Identity 服務的內容與特徵，希望能協助企業了解在不同的目標或情境之下，應如何挑選合適的 AD 防禦產品，以有效強化企業資安體質。

考量 AD 內的大量物件與其盤根錯節的關係，企業很難在不影響日常營運或系統運作的前提下，一次性排除掉所有的潛在威脅，因此我們建議您，在定期執行 XCockpit Identity 盤點可能遭利用的入侵路徑後，依據以下的威脅程度順序，逐一處理駭客更可能會利用的高風險目標、修正各項不安全的設定與弱點，定義出應優先守護的網路邊界：

- 全網域有關聯的特權群組
- 大量流通到各處的重點路徑
- 成本較小、較不易留下足跡的短路徑

最後，除了定期盤點 AD 資產外，也建議您進行持續性的安全態勢監控，如導入端點偵測與回應系統等，以利在瞬息萬變的資訊戰中免於蒙受損害。若您欲索取更多關於奧義智慧 XCockpit Identity 帳號安全態勢管理的規格或細節，或了解適合您企業的 AI 資安防禦解決方案，
請來信 contact-tw@cycraft.com。

關於奧義智慧 (CyCraft)

奧義智慧科技 (CyCraft Technology) 是一間專注於 AI 技術的資安科技公司，研發出自動化威脅曝險管理平台「XCockpit」，由獨家 Cyber x AI 技術針對端點安全、特權帳號、外部攻擊面等三大核心面向，提供視覺化的態勢管理介面與時時的攻擊面監測。

創立於 2017 年，企業總部位於臺灣，於日本、新加坡皆設有子公司，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，並受 Gartner、IDC 等世界級權威機構認可，選為 AI 資安報告之代表性案例企業，並曾多次斬獲海內外大獎肯定。

官方網站：https://go.cycraft.ai/web-zh


CYCRAFT