CYCRAFT
奧義智慧科技

產業客戶案例－金融業：全球人壽

雲端化與數位化的資安挑戰

金融機構如何確保與落實上雲後的資安需求？金管會於 2022 年頒布《金融資安行動方案 2.0》，訂定了 40 項措施、其中新增的資安措施就有 12 項，深化對金融業的資安規範，是全球第一個帶頭鼓勵產業擁抱「零信任框架」(Zero Trust) 的金融主管機關。針對雲端資安議題，金管會鼓勵金融機構加強其重要與核心資料保全機制，包含：核心資料檔案、資料庫加密與分持，儲存於第三地或雲端備份等機制。在金管會強化金融業者資安規範下，金融機構在具體操作上，有哪些資安產品或服務可用以事半功倍呢？這是金融產業的一大課題。

除此之外，自 2020 年起成立的保全／理賠聯盟鏈，利用區塊鏈技術、串接多家保險與壽險公司，有效達到跨公司的客戶資料交流。目前已有 20 多家壽險公司與數家產險公司加入聯盟，然而，不同公司的數位發展進程會直接影響資訊交換的流暢度與安全度。此數位轉型的種種嘗試：既存的紙本資料如何數位化、資料風險分級如何對接、自動化流程如何標準化等等，皆有賴資安解決方案提供穩固且可操作的框架。

全球人壽在臺灣有豐富的壽險經驗，近年來除了發展團體保險、銀行保險、保險經紀人代理人等多元化通路，也積極開發行動服務、線上平台、智能客服、 AI 分析客群大數據等科技業務。因應科技轉型與資安挑戰，全球人壽已在 2016 年導入 ISO 27001 國際資訊安全管理制度、於 2017 年獲得國際認證，並接續在 2017 年導入 BS 10012 個人資訊管理制度，更在 2022 年企業永續報告書中，將「資訊安全與客戶隱私」列為公司重要治理章節之一。

全球人壽資訊安全長暨副總經理林錦龍 (Alan Lin) 表示：「對於全球人壽的數位轉型業務，如：行動與遠距投保、行動理賠、行動保全等項目，我們首重的是資訊安全與客戶隱私保護，其次才是使用上的體驗要求」。金融業的根基為信賴，一旦客戶機敏資料外洩，損害不僅不易彌補、也將動搖客戶未來續約信心。全球人壽自 2022 年與奧義智慧合作至今，持續採用奧義智慧 Xensor MDR (雲端版)，由全球人壽資安同仁與原廠即時監控全場域端點、降低溝通與分析成本，產出多維度的威脅情資報告。

奧義智慧 XCockpit Enpoint 紅藍隊演練成效，精準分析帳號與設備信任度

在 2023 年底，全球人壽為驗證資安保護措施之有效性，同時回應金管會鼓勵金融機構偕同外部單位辦理聯合演練之要求，與奧義智慧合作進行了為期 45 天的紅藍隊演練。

此次演練期間，奧義智慧 XCockpit 自動化威脅曝險管理平台有效監控了 2,500 台電腦，成功偵測到 7 台紅隊活動，發出 275 封無誤報的告警通知，識別出 MITRE ATT&CK® 攻擊手法共 35 種，在平台上自動建立 35 筆工單。

XCockpit Endpoint 在全球人壽演練中，平均建單時間（MTTD）約 2 分鐘、平均分析時間（MTTI）為 12 分鐘，利用 AI 進行全場域分析時間則約為 37 分鐘，可快速梳理資安告警。

奧義智慧資安團隊參考 XCockpit Endpoint 報告後，藉由分析主要攻擊來源，奧義智慧建議全球人壽可以針對網頁的存取控制進行限制及落實 AD 的特權網域及高風險資源檔案盤點，以進一步強化管理措施。

XCockpit 平台針對 AD 帳號進行監管與分析，可自動關聯有加入網域的任何帳號與特性，包含使用者、群組、設備端點、組織單位（organization unit，OU）、群組原則（Group Policy Object，GPO）等，透過導入生成式 AI 、迅速關聯出所有端點的互動關係，利用資安情態圖掌握全場域潛在風險，並量化重要帳號或設備的可信賴程度。

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。

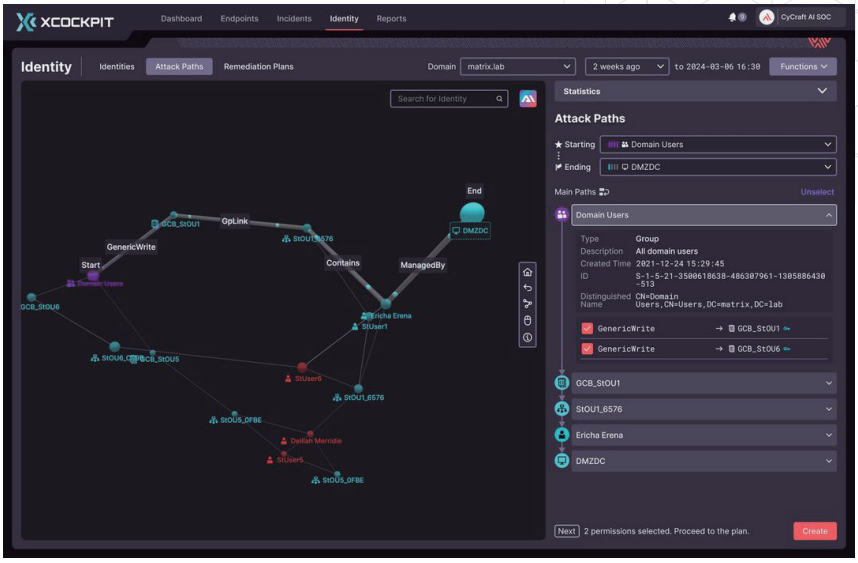
奧義智慧 XCockpit Identity 合規零信任安全框架，自動化與一站式管理資安挑戰

自 2020 年以來，美國、歐盟、新加坡、中國等國家陸續訂定了零信任網路安全策略，臺灣國家資通安全研究院亦於 2022 年發布政府零信任架構與相關規劃，逐步建立「身分鑑別」、「設備鑑別」和「信任推斷」此三大核心操作機制。金管會亦於 2024 年 7 月公告「金融業導入零信任架構參考指引」，鼓勵零信任網路部署，強調連線驗證與授權管控等機制之導入。金管會在參考美國網際安全暨基礎設施安全局 (CISA) 零信任成熟度模型、並依據我國金融業特性與其資安能量調整後，明確劃分四階段分級指標，依序盤點高風險場域之攻擊路徑，涵蓋身分、設備、網路、應用程式、資料等面向。

零信任架構導入過程中，不乏一定的風險與介接難題，根據奧義智慧在國內金融領域長期合作經驗，我們觀察到客戶多半擔憂因人員不熟悉相關設定、運作或進行錯誤的組態配置，導致整個組織營運不穩定。奧義智慧 XCockpit 平台之 Identity 模組可協助客戶進行場域內外部衝擊性分析，找出同時具備高風險與低衝擊性場域，讓組織在嘗試新科技時，亦能免於遭受嚴重衝擊。

在測試與執行 XCockpit Identity 後，資安長林錦龍副總經理表示：「XCockpit 平台透過盤點五大資源存取途徑，以及整合 FIDO 身分鑑別，提供了我們設備鑑別評估、外部曝險評估、高權限風險評估等決策資訊，不僅有利於動態管控存取安全，也是金融產業在適用零信任框架上的一大助力。」

由此可見，資安產品與服務不僅可守（協助金融機構合乎法遵規範）、更加可攻（積極導入零信任安全框架）。奧義智慧 XCockpit 平台以生成式 AI 自動化偵測、監控與分析新型態資安挑戰，整合 Endpoint 端點安全態勢管理、Identity 帳號安全態勢管理，一站式管理各曝險面向，降低資安維運成本、提升管理效率，更為金融產業數位轉型奠定穩固基礎。



「XCockpit Identity 帳號安全態勢管理平台」提供可視化的攻擊路徑模擬，為企業自動找出需優先處理的「攻擊最短路徑」。
*示意圖內容僅為產品展示，所有數據及資料均與客戶無關。

全球人壽與奧義智慧資安防護三大要點：

1. 因應金融業的高槓桿產業特性，快速提供精準的分析報告、避免告警疲勞，並回應高規格的主管機關稽核要求。
2. XCockpit 自動化威脅曝險管理平台監管與分析 AD 場域內的身分與設備，為未來零信任架構規範的設備鑑別與信任推斷鋪路。
3. 資安產品與服務打造的安全穩定網路框架，為金融機構邁向數位轉型、發展多元雲端服務，奠定穩固基礎。

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