



核心團隊

我們的核心團隊由多位深耕資安、研發與系統整合領域的資深專家所組成。擁有跨足產業與技術的實戰經驗，具備強大的策略規劃與技術落地能力。他們長期服務於企業與政府單位，精通資安法規、標準與最佳實務，並曾主導多項大型專案的安全架構設計與風險評估。

團隊累積超過 20 年的系統整合與技術服務經驗，熟悉多元產業環境，擅長從需求分析到方案交付的全流程管理，能夠將實際環境需求做為導向，轉化為可行且具市場競爭力的技術解決方案。團隊具備以用戶視角切入技術開發的能力，確保產品不僅創新，更貼近客戶實際需求與預算。

在推動公司發展的過程中，我們將AI與自動化視為產品核心，致力於在技術創新與實務應用間取得最佳平衡。首創產品以「組態管理」為切入點，未來也將擴展至更多資安場景，打造兼具深度與彈性的智慧解決方案。

願景與使命

願景 (Vision)

我們深信，人工智能時代的來臨，將徹底改變企業防禦威脅的方式——從被動補漏洞，轉向主動偵測、預防與自動化修復。未來，資安不再只是一組機制，而是結合大數據分析、機器學習、巨量運算的動態系統。

「AI x 資安管理」將成為企業達到零信任 (Zero Trust) 與動態防護的必備思維，協助組織在高度變動的網路環境中保有持續安全。

使命 (Mission)

以創新驅動，利用最前沿的機器學習與深度學習技術，將複雜的資安機制與數據處理流程自動化、可視化，讓資安做到合規、安全、輕鬆。

深度市場調研與多元產業經驗為基礎，針對金融、政府、製造、醫療、等不同產業之風險特性，量身設計合適的 AI 驅動資安方案。未來在產品設計上，都會以模組化、可拆分、易整合的方式，支援客戶按需求自由擴充為最優先考量。

未來展望

在 AI 重塑所有產業運作邏輯的時代，每一個系統、每一項產品，甚至每一個本來「運作正常」的流程，都值得被重新定義一次。效率、精準、彈性，已經從選項變成了基本條件。我們相信，AI 不只是資安工具的一部分，我們正在打造的，是一個由 AI 驅動、走在前線的資安系統。

因為我們使終相信，在 AI 應用時代，現有的產品和商業需求，都值得結合AI工具，再開發一次。



安睿資安股份有限公司

地址：104南京東路二段150號225室

電話：02-2506-0501

Mail：service@en-radiant.com.tw



Line

安睿資安股份有限公司



AI x 資安管理

打造更全面高效的完整資安體系



智能化



動態化



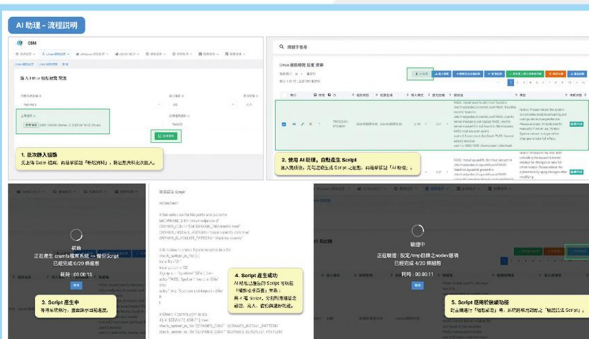
場景化擴充

自 2024 年起本公司開始進行資訊安全解決方案的技術研發與市場規劃，立足於「AI x 資安管理」的核心理念，目標是以人工智能驅動、數據思維為基礎，打造更全面且高效的資安服務。經過一年多的技術驗證與策略討論，我們於 2025 年 5 月正式成立。我們率先推出首支聚焦「組態管理」的產品，並以之作為切入點。未來我們將持續擴展到更多資安領域，以AI技術為驅動，實現「智能化、動態化、場景化擴充」的完整資安體系。



什麼是 CBM?

CBM，全名為「組態設定基準管理 (Configuration Baseline Management)」，顧名思義，是為了解決市面上組態管理工具僅能依制式模板做到合規，但無法因應組織真實需求而產生的。不同於市面上只能針對 TWGCB、FCB 等標準進行模範化套用的產品，CBM 更進一步提供高度自定義的能力，讓使用者不只能依據法規設定組態，還能從已有標準文件的組態管理中自由挑選、建立屬於自己組織情場的資安規範。CBM 的價值，在於它不只是為你套合規模板，而是讓你定義真實場景需求，把組態管理真正落實到組織獨特的業務邏輯與資安策略之中。



組態管理 x AI = 效率+告別條條框框的限制

只需導入CBM組態基準管理，我們的AI系統便能運用LLM（大型語言模型）快速自動生成符合TWGCB/FCB標準的腳本，節省高達90%的時間，合規就是那麼輕鬆。AI x 高度自由的自定義組態管理，告別市場定制化產品的棄白，讓組態設定都能真正對應你組織的場景與策略需求。



零基礎也能輕鬆駕馭 組態管理從未如此簡單

別擔心技術門檻，不會AD導入、不懂指令、不熟腳本的小白也能輕鬆上手。CBM的組態管理操作簡單，我們將複雜的組態管理變得直觀又自動化，即使是新進的員工，也能完成過去要工程師花好幾小時才能搞定的設定，輕鬆合規TWGCB/FCB。



全方位組態標準 一站整合，立即應用

我們內建一套標準多標準組態知識庫，涵蓋全球主流安全基準，讓您在設定上不再從零開始。整合Admx/Adml、STIG (美國國防部)、CIS Benchmark (國際資訊安全標準)、TWGCB (台灣組態基準)、FCB (金融業組態基準) 等權威規範，讓您可以取得最佳組態設定建議。支援多平台：涵蓋 Windows、Linux、Unix、網路設備與應用程式。你的資訊環境再複雜，也有標準可循，組態設定，從此更聰明、更安心。



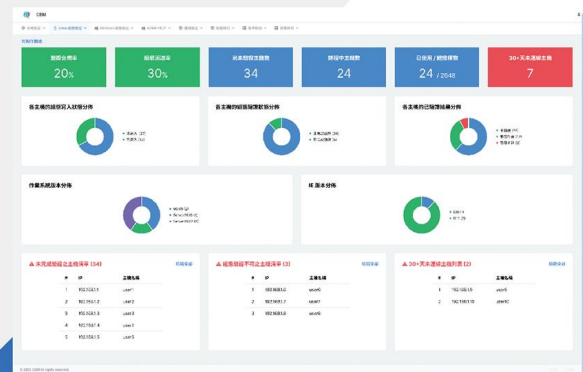
介面直覺、管理簡單 全面掌握組態狀態

從操作體驗到報表產出，我們重新定義資安管理的使用門檻。透過精心設計的UI介面與智慧儀錶板，任何人都能快速上手，即時掌握全局。報表查看結果，呈現自動比對組態設定是否成功、例外管理機制，滿足各別單位使用的特需場景需求，同時例外管理設置強制記錄原因，再久也能找回原因，系統還原功能，每次變更都可回滾，風險降到最低。套用報表產出，一鍵生成符合稽核需求的標準報告，支援導出與儲存。



彈性部署 輕鬆整合你的IT環境

無論你的環境偏好Agent-based，或是偏好免安裝SSH-based模式，我們都支援。我們提供雙模式部署架構，讓你根據系統需求與安全策略，自由選擇最適合的整合方式。



不只「合規」 更能「超前部署」

透過CBM組態基準管理系統，你能更有效控管資安風險，快速識別異常設定，避免潛在漏洞。在全面符合 GCB / FCB 法規規範同時，自動對照，降低稽核壓力。合規只是開始，超越合規的自定義防護需求，不間斷的持續防禦，才是你超前的資安策略。



高度自由自定義 白話CBM為你的複雜情境而生

我們的系統具備高度自由的自定義能力，能按圖勾選你要的組態設定。完美支援不在基準範圍內的各類組態情境，不管流程再複雜，AI 都能幫你搞定。我們不只解決常見合規問題，我們打造屬於你的解方。我們深知，每一家企業的組態管理需求都獨一無二。TWGCB / FCB 的合規只是起點，真正重要的，你的場景需求才是終點。