

人機協作： **Agentic AI** 如何協助精實安全團隊

本白皮書是關於 Agentic AI 的入門指南，說明具備自主性與情境感知能力的數位助理如何幫助 SOC 團隊更有效率地檢測、調查和回應威脅，並在與人類分析師協作的過程中持續學習與進化。

引言：Agentic AI 在資安領域的崛起

在現今的資安環境中，威脅的數量、速度與複雜性早已超越多數 SOC 的應對能力。尤其對於中型企業而言，他們不僅要面臨資源有限、分析師過勞日益嚴重的挑戰，還要保持企業級的威脅防禦力。**Agentic AI** 因此應運而生——這類全新的 AI 助理不會取代人類分析師，而是成為不知疲倦的數位工作夥伴，強化他們的能力與效率。

Agentic AI 的出現，代表資安自動化技術的一大躍進。它賦予資安團隊具備智慧、目標導向的代理角色，能自主決策、理解情境，並持續學習進化。本文將深入探討什麼是 Agentic AI、其建構方式，以及它如何在各種應用情境中帶來實質的效率提升，特別是人力有限的 SecOps 團隊。

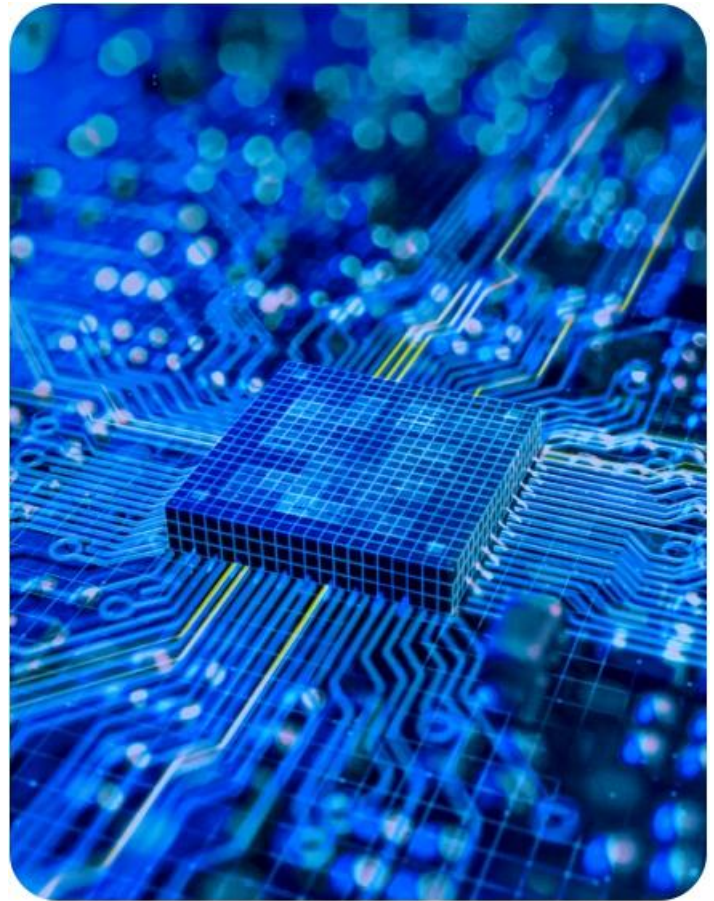
什麼是 Agentic AI？

Agentic AI 指的是能在動態環境中**感知、推理、決策並採取行動**以達成特定目標的自主軟體實體。不同於以規則為基礎的自動化或傳統的端點代理程式，**Agentic AI** 能夠獨立運作，具備即時情境理解能力，且透過持續學習循環不斷進化。

Agentic AI 的關鍵屬性包括：

- **自主決策**：無需人工持續監督即可做出決策並採取行動。
- **情境推理**：能理解環境中的細微差異，並依此調整行為。
- **多重步驟任務執行**：能將複雜的操作（調查、關聯、回應）串接成策略性工作流程。
- **回饋學習**：透過成功經驗、錯誤與手動回饋中持續學習、優化。

在 SOC 中，這意味著代理不僅僅是記錄警報，而是能**主動偵測威脅、調查根本原因、執行回應並持續優化策略**，這一切都能在不佔用分析師大量心力的情況下完成。



Agentic AI 的建構方式

Agentic AI 仰賴多項先進技術的整合：

- **大型語言模型 (LLM)**：自然語言理解與決策邏輯的基礎。
- **強化學習 (RLHF)**：透過嘗試與回饋的方式訓練代理角色來優化行為，並由人類分析師引導學習方向。
- **生成式 AI**：可動態產出事件摘要、風險報告與事件回應劇本等內容。
- **資安領域知識**：融合來自身分、端點、雲端和網路安全工具的專屬資料。
- **整合框架**：可與現有的 SIEM、XDR、SOAR 及工單系統互通運作，確保流程執行順暢。

這些元件相互結合，造就出能根據業務和資安優先事項進行協作決策的數位工作夥伴。

Agentic AI：幫助您，而非取代您

與許多人對 AI 取代人類的憂慮相反，Agentic AI 旨在「輔助」，而非取代資安分析師。您可以把它想像成一位虛擬的一線分析師，它永遠不會疲倦、不會忽略各種情境細節，並能隨著工作量彈性擴充。

以下為 Agentic AI 如何成為您值得信賴的資安夥伴：

- **提升分析師生產力**：代理角色處理繁瑣的重複性任務，讓人類分析師能專注於威脅獵捕、事件分析與策略規劃。
- **減少警報疲勞**：自動篩選與排序事件，僅顯示真正重要的威脅。
- **累積組織知識**：從過往的應變經驗中學習，加速未來調查流程，建立組織記憶。
- **協同式自主運作**：代理角色具備獨立執行能力，但人類分析師仍可參與其中，進行監控、調整與升級。

最終成果是打造出一個更具彈性、以人為本的 SOC—更快、更聰明、更不容易倦怠。



使用案例：Agentic AI 在精實 SecOps 團隊中的實際運作



1. 自主威脅偵測與回應

Agentic AI 能從多個遙測來源（雲端、端點、身分與網路）收集警報並即時進行關聯分析。該代理程式不會將大量原始資料堆給分析師，而是自行判斷是否為惡意行為，並回應與記錄原因。

提高生產力：可將威脅偵測到回應的時間縮短高達 **90%**，每週為分析師節省 **10 - 15 小時**。



2. 智慧警報分類與調查

Agentic AI 不再將成千上萬的警報直接丟給分析師處理，而是根據風險情境進行優先排序、主動調查異常行為，並為每則警報補充相關證據、影響程度與可信度資訊。

提高生產力：可減少 **70 - 80%** 的警報分類時間，讓團隊每天能夠處理 **4-5 倍以上的威脅**。



3. 具學習能力的動態回應劇本

Agentic AI 能依據即時評估結果，自動執行多重回應，例如隔離端點、停用帳號、封鎖 IP 等。此外，它也會根據分析師的回饋持續學習，調整後續行動，降低誤判風險。

生產力提升：將手動維護回應劇本的需求最小化、持續優化，且無需仰賴工程團隊持續支援。

對精簡安全團隊的預期效益

對人力有限的中小型組織而言，Agentic AI 可顯著提升營運效率：

	使用 Agentic AI 前	採用 Agentic AI 後
分析師 每週工作時間	40-50	20-25
平均檢測時間 (MTTD)	從幾小時到幾天	幾分鐘
平均回應時間 (MTTR)	幾小時	幾分鐘
每月事件處理量	100-150	300-500
警報疲勞	高	顯著減少

整體而言，組織可以預期**整體生產力提高 30-50%**，讓現有團隊無需增加人力，就能專注於高價值任務和策略成果。

中型企業市場的自治之路

對某些中型企業而言，要實現完全自治的 SOC 可能遙不可及，但 Agentic AI 正讓這個目標變得觸手可及。它無需龐大的預算或全天候的人力，而是透過強化現有工具



與人員能力，即時帶來投資回報，並提供可持續擴展的自主性發展路徑。

透過這種方式，Agentic AI 不僅可以保護您的基礎設施，更是在資安戰場上創造公平競爭的機會，讓中型團隊也能實現企業級的資安防護成果。

結論：Agentic AI 是安全協作的未來

資安挑戰不會消失，但藉助 Agentic AI，精實安全團隊能正面迎戰——決策更迅速、疲勞感降低，處理精準度也大幅提升。

這不是「人類對抗機器」，而是「人機協作」的全新局面。

Agentic AI 可賦能分析師、重塑資安營運流程，並引領至更自主的未來。對於具前瞻性思維的資安團隊來說，導入 Agentic AI 的最佳時機不是「未來某天」，而是「現在」。

關於代理商 **SPHINXTEC 欣盟科技**
all about data security

欣盟科技 (SphinxTec Co., Ltd.) 以專業的技術服務為基礎，遵循資訊安全的規範，我們以守護客戶的資訊為首要考量，代理銷售不同領域之領導品牌，協助客戶在駭客攻防之中提早預防取得先機，且以欺敵技術降低駭客攻擊突破率，打造堅韌的資安防護網。欣盟科技亦提供資安技術顧問服務可客製化企業需求去分析找出關鍵核心，提供適切的資安策略，配合使用實際的可行性分析，導入適合的企業資安解決方案。