

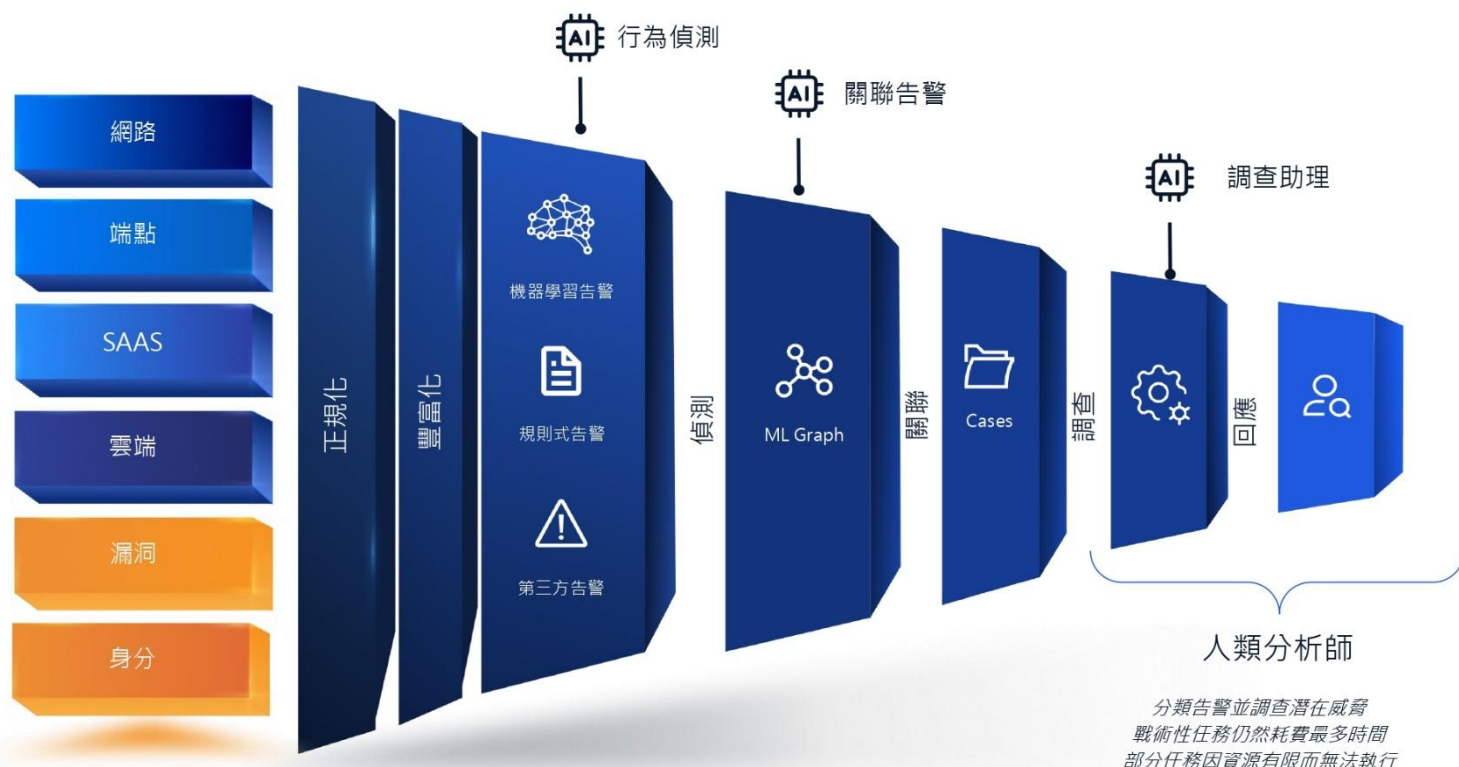
Stellar Cyber：AI 原生 SecOps 平台

與 Stellar Cyber 一起踏上人類增強自主化 SOC 之旅

與傳統僅收集日誌、讓分析師疲於應對海量日誌的傳統 SIEM 不同，Stellar Cyber 是唯一專為 MSSP 與企業安全團隊打造的 AI 原生 SecOps 平台。

於單一授權下整合 SIEM、NDR+、ITDR、TIP、UEBA 及多層式 AI™ 技術，提供統一的威脅可視性與自動化分析能力，協助企業看見潛藏於複雜環境中的資安威脅，消除資料孤島、降低營運複雜度，同時大幅提升事件偵測與回應效率。

傳統 SOC	Stellar Cyber
手動、被動式威脅偵測	AI 驅動的主動式安全自動化
複雜且各自獨立的資安工具	整合 SIEM 、 NDR 與 XDR 的統一平台
人工調查耗時費力	自動事件關聯與回應
分析師被海量告警淹沒、陷入告警疲勞	透過智慧自動化分類與 AI 驅動的威脅調查，減輕人力負擔
對威脅的反應鈍化減慢	即時、AI 驅動的威脅遏制





AI 驅動的威脅偵測

發揮次世代 SIEM、NDR 與 Open XDR 綜效，減少警示疲勞，並即時揭示真實威脅。



完整的攻擊面可見性

即時監控雲端、端點、網路、IoT 環境，將來自多個來源的日誌、警報與遙測數據標準化並加以分析，不輕忽任何安全漏洞。



自動分類與優先排序

透過多層式 AI™ 自動關聯相關事件，並分類成高可信度事件，簡化事件應變流程，縮短平均偵測時間 (MTTD) 與平均回應時間 (MTTR)。



自動化事件回應

透過內建或客製化劇本自動回應，快速遏止威脅，如：封鎖網域、隔離主機、註銷帳號。



與現有工具完美整合

開放架構支援 SOAR、EDR、威脅情報串流及任何第三方安全解決方案，讓資安團隊能靈活客製化工作流程並擴展威脅偵測能力。

為什麼選擇 Stellar Cyber ?

攻擊趨勢顯示，駭客的攻擊速度持續加速，並可在數分鐘內跨越端點、身分、SaaS、OT 與雲端 API，各自孤立的資安工具很難捕捉這些變化。SIEM 曾試圖解決這個問題，但成效有限；後來外加的機器學習與 SOAR，也多半只能在告警觸發後被動回應。直到 XDR 式的整合架構與多層式 AI 出現，才真正改變了遊戲規則——僅有 Stellar Cyber 打造出能將這一切完整串聯的平台。

透過 Stellar Cyber，您將獲得：

- 在資料匯入當下即進行更早期的威脅偵測，而非數小時後。
- 透過跨領域關聯分析，建立更完整且有強而有力的事件脈絡。
- 由多層式 AI 驅動，大幅加速調查流程。
- 自動化回應機制，即時降低風險。
- 充分發揮既有資安工具的效益，獲得真正的投資報酬率。



代理商 欣盟科技有限公司

SPHINXTEC 欣盟科技

all about data security

Tel: 03-6682708

<https://www.sphinxtec.com/>

CustomerCare@sphinxtec.com